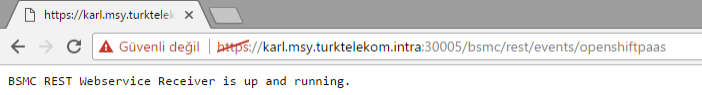
**WEBHOOK OPENSHIFT ALARM ENTEGRASYONU GEREKSİNİMLERİ**

Webhook POST metoduyla request göndereceğiniz sunucunuzdan aşağıdaki hostname ve porta erişimi açtırılması gerekmektedir.  
  
Source name : Webhook sunucusu  
Destination name : karl.msy.turktelekom.intra/10.6.102.180  
Port: 30005 TCP Çift Yönlü  
  
**POST metoduyla request göndereceğiniz URL bilgisi :** [https://karl.msy.turktelekom.intra:30005/bsmc/rest/events/<uygulama\_ismi](https://karl.msy.turktelekom.intra:30005/bsmc/rest/events/%3cuygulama_ismi)>

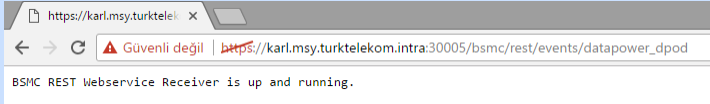
* **Uygulamanız Bulut Platformları Oper. Müdürlüğünün sorumluluğundaki Openshift ortamında bulunuyorsa** ekstra firewall erişimi almanıza gerek yoktur. Menderes Keskin veya ekip arkadaşından destek alıp alarm testleri gerçekleştirilebilir.

Endpoint URL : <https://karl.msy.turktelekom.intra:30005/bsmc/rest/events/openshiftpaas>



* **Uygulamanız kendi Openshift ortamınızda bulunuyorsa** yukardaki firewall erişimlerinin alınmasının ardından POST metoduyla göndereceğiniz web requestin JSON tipinde dosya iletmeniz gerekmektedir. Arakatman Operasyonları ekibiyle yapılan örnek çalışma aşağıdaki gibidir. Bu çalışma referans alınabilir.

Endpoint URL : <https://karl.msy.turktelekom.intra:30005/bsmc/rest/events/datapower_dpod>

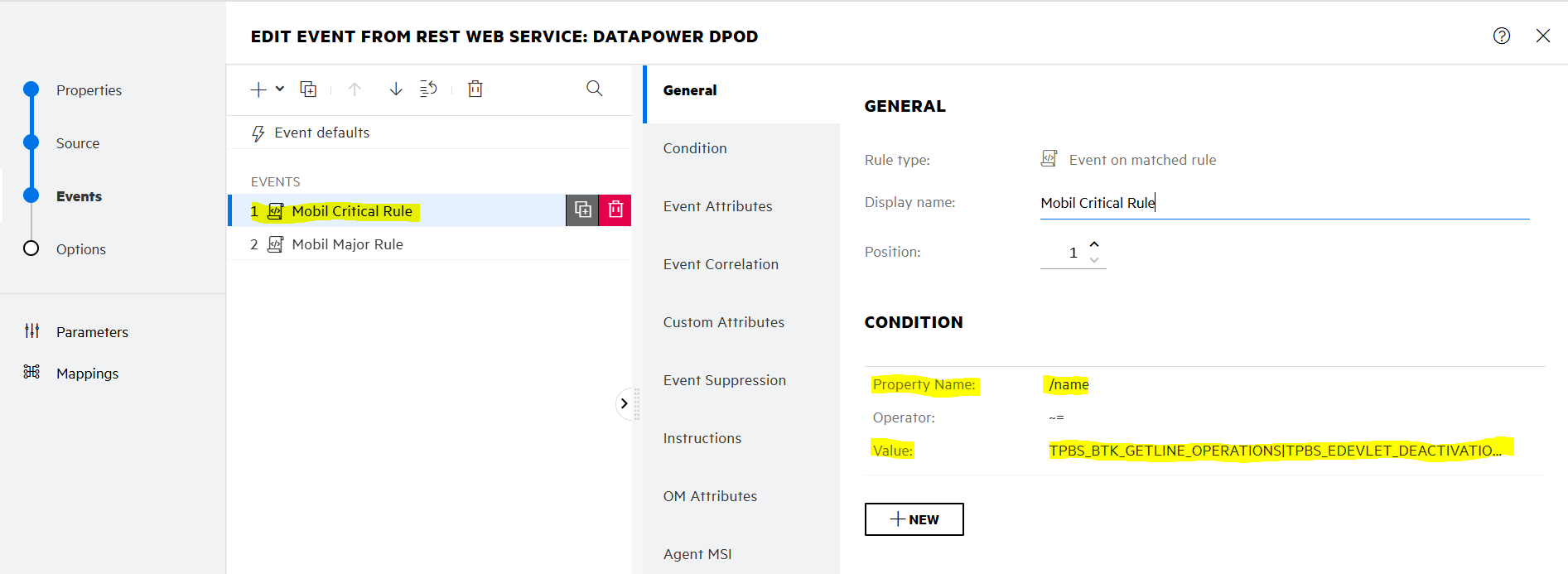


**İletilen veya sonradan oluşturulan json dosyası :**

****

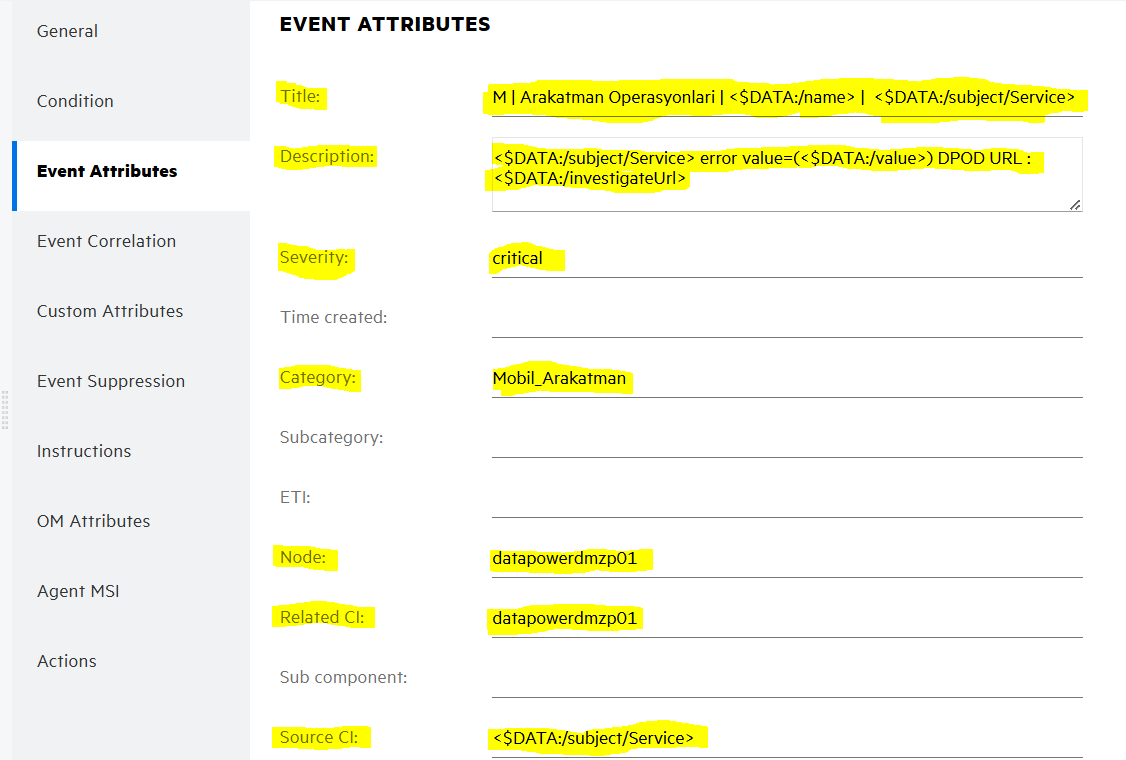
**JSON DOSYASIYLA BERABER OLUŞTURULAN POLICY VE MAPPINGLER**

* Kuralda ilk olarak “Condition” alanında Property Name alanında hangi ifadenin geçeceği belirtilmelidir. Aşağıda örneğin /name alanı baz alınmış. Ya da /alerts/status alanında “firing” ya da “resolved” geçmesine bağlı da condition oluşturulabilir.



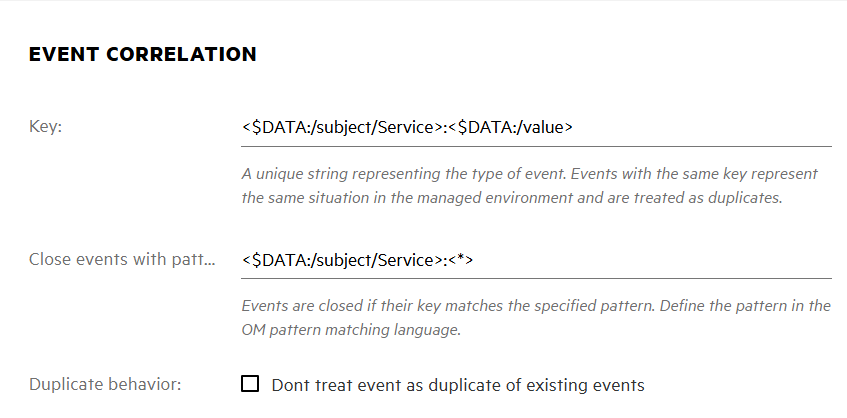
**EVENT ATTRIBUTES**

* Title alanına alarmın başlığı nasıl olması gerekiyorsa “Company | Grup İsmi | ham veride olması gereken alarmlar” olarak düzenlenir. Sabit domainler için Company:F; Mobil domainler için Company:M; Genişbant domainler için Company:B olarak girilir.
* Description alanına ham veride olması gerekenler veya tüm veri yazılabilir.
* Severity alanına alarmın severity bilgisi girilir.
* Category alanına Opsbridge alarm notifikasyonun çıkacağı mail adresleri ve SMS numaralarına bağlı olarak mesaj grup veya diğer adıyla kategori bilgisi girilir.
* Node ve Related CI alanlarına alarmın yapışacağı CI bilgisi girilir. Aşağıdaki örnekte CI bilgisi manuel girilmiştir. Ancak ham veride bu alan gönderiliyorsa(örneğin; <$DATA:/alerts/0/labels/relatedci>) gibi bir alan da yapıştırılabilir.
* Source CI alanına ham verideki bir alan ya da manuel bir isim girilebilir.

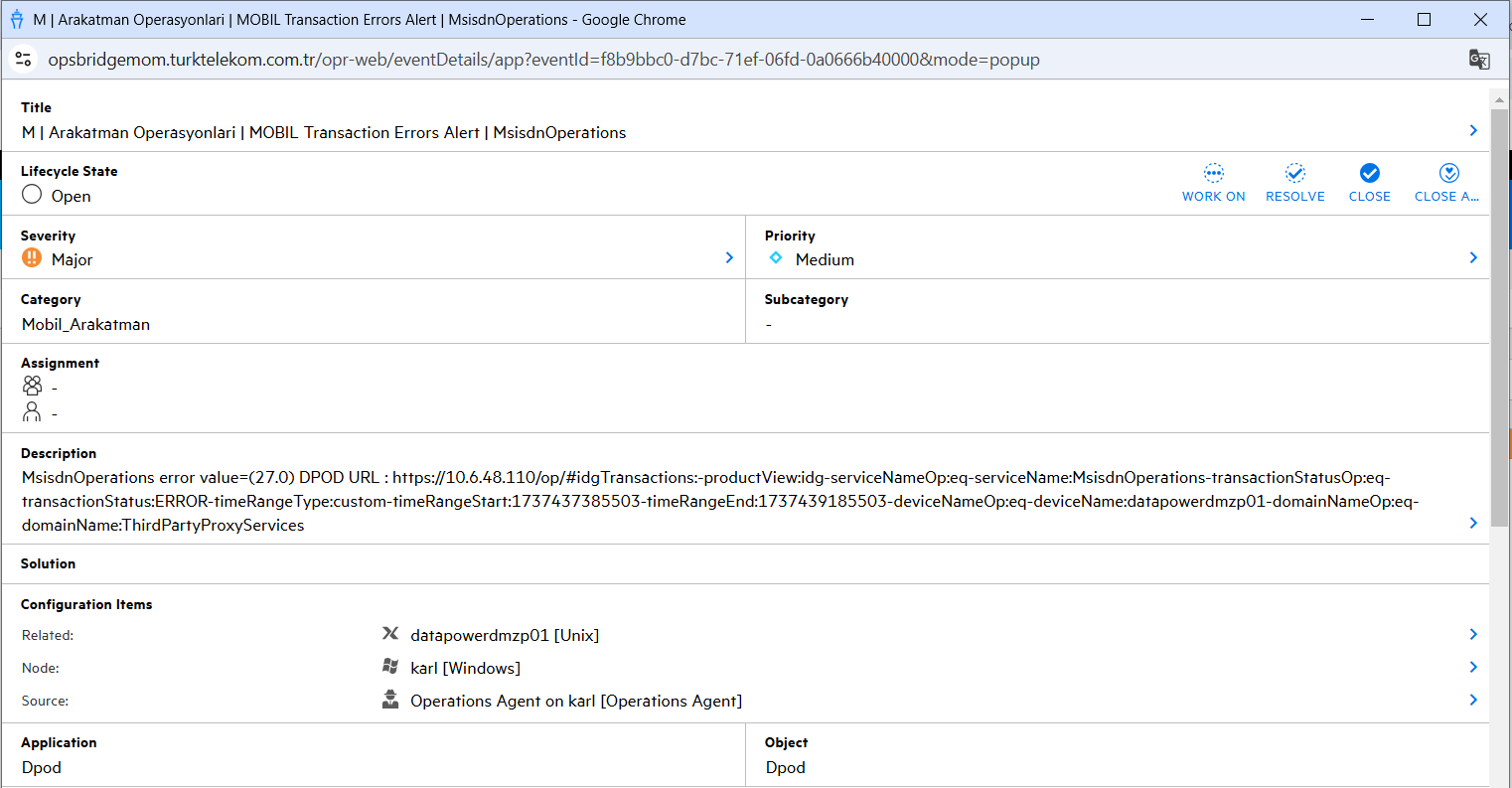


**EVENT CORRELATION**

* Alarm korelasyon alanında trigger olan alarmın nasıl clear olacağı veya nasıl duplike olacağını gösteren kuraldır. Burada girilecek ham verideki alan unique olmalı ve diğer alarmlardan ayrıştırılabilir olmalıdır.



**ÖRNEK OPSBRIDGE ALARMI**



**Original Data:**

[{

"uuid": "8065af0d-6291-4598-92c5-d6ebf1ea57d4",

"environment": "dpod",

"name": "MOBIL Transaction Errors Alert",

"type": "Frequency",

"timeIntervalStart": 1737437385503,

"timeIntervalEnd": 1737439185503,

"creationTime": 1737439209833,

"value": "27.0",

"threshold": 15.0,

"subjectTerms": "ObjectType=wsgw, Service=MsisdnOperations",

"subjectKey": "wsgw MsisdnOperations",

"investigateUrl": "https://10.6.48.110/op/#idgTransactions:-productView:idg-serviceNameOp:eq-serviceName:MsisdnOperations-transactionStatusOp:eq-transactionStatus:ERROR-timeRangeType:custom-timeRangeStart:1737437385503-timeRangeEnd:1737439185503-deviceNameOp:eq-deviceName:datapowerdmzp01-domainNameOp:eq-domainName:ThirdPartyProxyServices",

"subject": {

"ObjectType": "wsgw",

"Service": "MsisdnOperations"

},

"description": "An alert of MOBIL Transaction Errors Alert has been generated for ObjectType wsgw, Service MsisdnOperations"

}]

* Application ve Object alanlarına mail notifikasyonunda da gözükecek olan uygulama ve obje isimleri girilir.

